A GOVERNMENT TECHNOLOGY THOUGHT LEADERSHIP PAPER | AWS AND CROWDSTRIKE

3 cybersecurity steps that small and mid-sized governments should take

Introduction

Cyberattacks are especially intrusive for small and mid-sized local governments. A water services agency, for instance, could be easy prey for criminal gangs and nation-state actors. Even if services aren't interrupted, agencies must devote scarce resources to keep intruders out of their systems.

A July 2024 Center for Digital Government (CDG) survey underscores the security challenges of mid-sized agencies. Nearly two-thirds of respondents called rapidly evolving threats their top security issue. The survey's results also point to a critical three-pronged strategy: identifying your top security challenges, setting investment priorities, and joining forces with statewide cyber defense efforts.

Nearly two-thirds of respondents called rapidly evolving threats their top security issue

1. Assess your top cybersecurity challenges

Cybercriminals do not spare smaller cities, counties and similar jurisdictions. Attacks on water systems in Texas[1] and Kansas[2] in 2024, for instance, forced officials to put operations in manual mode while cyber experts sorted things out. Hackers linked to Russia were among the suspected culprits. The water kept flowing, but the implication was clear: No jurisdiction is safe, so cyber preparation is essential for all.

“You can’t afford to not do anything,” says Maria Thompson, executive government advisor with Amazon Web Services (AWS).[3]

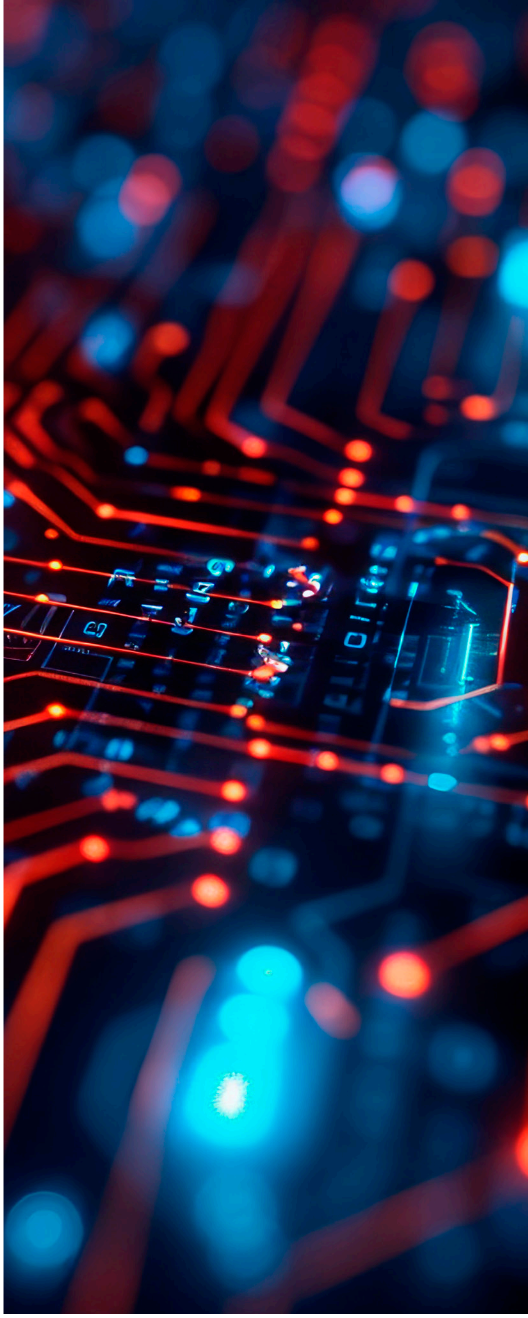
Your agency should do the following to prepare:

Face the risks. The volume of cyberattacks continues to increase every year. Intruders’ breakout speed, which tracks how long they take to infest a system after sneaking in, is rapidly accelerating. A half-dozen years ago, average breakout speed was just under 10 hours, according to Matt Singleton, executive strategist with CrowdStrike, a leading provider of intrusion detection-and-response solutions. Last year, CrowdStrike noted it had shrunk to 62 minutes.[4] “The fastest time we’ve seen is 127 seconds,” Singleton says.

Automate. Use automation and AI-driven technologies to streamline your security operations to detect and respond to threats faster.

Ready your tools. Assess your risk landscape and inventory your cyber defense software arsenal. An inventory can help agencies identify effective cybersecurity software tools they aren’t using. Moreover, tools can often be consolidated.

Expect more ransomware. Cyber extortion threats aren’t going away. Most successful breaches result from credentials harvested by phishing and other tactics. Make sure you have tools to address identity protection, disaster recovery, device monitoring, and detection/response.

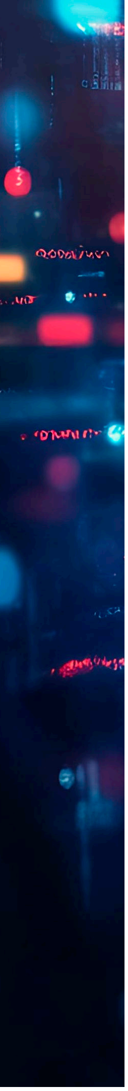


Top five cyber challenges for mid-sized governments

1. **Rapidly evolving threats 62%**
2. **Limited budget/resources 53%**
3. **Outdated technology/systems 45%**
4. **Insufficient cybersecurity staff and training 38%**
5. **Vendor/cloud security concerns 24%**

Source: Center for Digital Government. Mid-Sized Cities and Counties Survey. July 2024.

Use automation and AI-driven technologies to streamline your security operations to detect and respond to threats faster.



2. Identify where you need the most investment

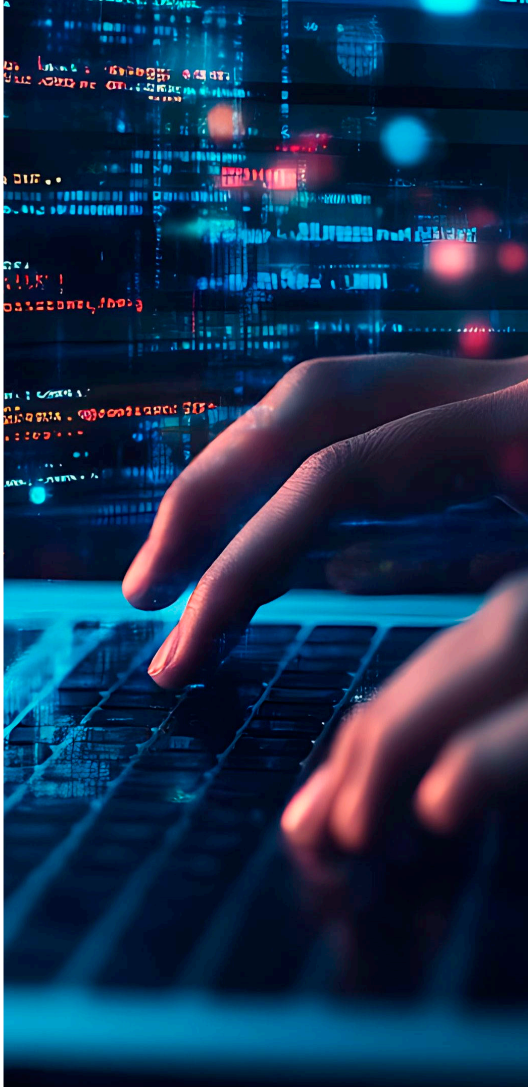
Every government must assess its knowledge, skills, and tools to achieve system-specific security goals. The following tips will help you make the right investments:

Strengthen culture. While people often pose the most common vulnerabilities, they also can be the strongest defenders — if the agency supports a security culture. “Let’s build cybersecurity into the mindset of every person in the organization,” Singleton says. After all, people can face cyberattacks in their personal lives as well. When that happens, it’ll have an impact in the workplace. If you’re short-staffed, take advantage of managed security services.

Train your people. Make sure everybody has a grounding in cyber fundamentals. Online courses can help staff learn at their convenience. Don’t skip training when you acquire new security tools — they’re not much use if your staff doesn’t know how to use them.

Strike a balance. IT leaders must dovetail human, technical and process issues to avoid overemphasizing one area and creating problems somewhere else. Take time, for instance, to ensure every new tool is properly implemented. “If it’s not configured correctly, it’s just another risk to your environment,” Thompson says.

Get funding. Apply for cyber grants while they’re still available. Thompson notes that about $280 million is in the federal cybersecurity grants pipeline for state and local governments.

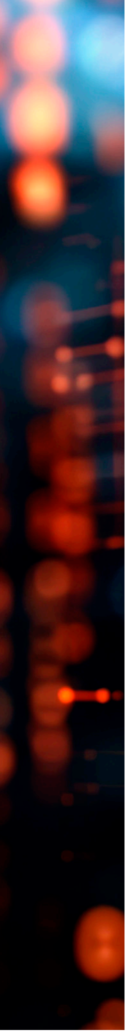


Top five cyber weaknesses for mid-sized governments

1. **Employee training and awareness 60%**
2. **Advanced threat detection and prevention 53%**
3. **Network security 45%**
4. **Enhancing identity protection and access management 43%**
5. **Incident response and recovery 41%**

Source: Center for Digital Government. Mid-Sized Cities and Counties Survey. July 2024.

Don’t skip training when you acquire new security tools — they’re not much use if your staff doesn’t know how to use them.



3. Embrace Whole-of-State Security

Whole-of-state security is an emerging strategy that connects cities, towns and counties with the security resources of their state governments.[5] This “all hands on deck” approach pools resources and enables smaller jurisdictions’ teams to explore options like teaming up with cyber defense experts in their state’s National Guard. The CDG survey found that 22% of respondents didn’t know whether they were in a whole-of-state program. If you’re unsure of your whole-of-state status, contact your state’s chief information security officer and find out how to participate.

Action items:

- **Team up.** Find collaboration partners in the private and public sectors that can help address cyber threats. Agencies seeking cybersecurity grants stand a better chance of landing recurring funding if they can demonstrate they’re collaborating at an ecosystem level to reduce security risks.
- **Do your homework.** Track down statewide cyber defense initiatives and explore how you can participate.
- **Start right away.** There’s no time to lose in this environment. To get moving on whole-of-state protection, smaller jurisdictions may have to overcome their anxieties about state agencies having access to their network environment, Thompson says.

Top five actions by mid-sized governments moving toward whole-of-state approach

1.	Conducting internal assessments and evaluations	46%
2.	Engaging in discussions with state cybersecurity authorities	39%
3.	Participating in state-level cybersecurity training and awareness	38%
4.	Integrating state cybersecurity policies and standards	30%
5.	Applying for state funding or resources for cybersecurity initiatives	29%

Source: Center for Digital Government. Mid-Sized Cities and Counties Survey. July 2024.

Find collaboration partners in the private and public sectors that can help address cyber threats.

1. https://www.texastribune.org/2024/04/19/texas-cyberattacks-russia/
2. https://www.darkreading.com/ics-ot-security/kansas-water-plant-pivots-analog-cyber-event
3. https://webinars.govtech.com/Keeping-Your-Mid-Size-Government-Agency-Resilient-and-Secure-142850.html
4. https://www.crowdstrike.com/resources/reports/threat-hunting-report/
5. https://www.govtech.com/security/whole-of-state-cybersecurity-gains-ground-in-government

This piece was written and produced by the Government Technology Content Studio, with information and input from AWS and Crowdstrike.

Produced by Government Technology
Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com

Sponsored by AWS
Amazon Web Services (AWS) Worldwide Public Sector helps government, education, and nonprofit customers deploy cloud services to reduce costs, drive efficiencies, and increase innovation across the globe. With AWS, you only pay for what you use, with no up-front physical infrastructure expenses or long-term commitments. Public Sector organizations of all sizes use AWS to build applications, host websites, harness big data, store information, conduct research, improve online access for citizens, and more. AWS has dedicated teams focused on helping our customers pave the way for innovation and, ultimately, make the world a better place through technology.

To learn more about AWS in the public sector, visit us at **aws.amazon.com/stateandlocal.**

Sponsored by Crowdstrike
CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints, cloud workloads, identity, and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft, and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting, and prioritized observability of vulnerabilities. Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity, and immediate time-to-value.

Learn more: **https://www.crowdstrike.com/**

ADOBESTOCK/AI GENERATED